European Parliament
2014-2019

TEXTS ADOPTED

P8_TA(2017)0076

Fundamental rights implications of big data

European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))

The European Parliament,

– having regard to Article 16 of the Treaty on the Functioning of the European Union,

– having regard to Articles 1, 7, 8, 11, 14, 21, 47 and 52 of the Charter of Fundamental Rights of the European Union,

– having regard to the guidelines for the regulation of computerised personal data files of the United Nations General Assembly in its Resolution 45/95 of 14 December 1990,

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1] (GDPR), and to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[2],

– having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled ‘A Digital Single Market Strategy for Europe’ of 6 May 2015 (COM(2015)0192),

– having regard to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981 (ETS No 108) and its Additional Protocol of 8 November 2001 (ETS No 181)[3],

---

1 OJ L 119, 4.5.2016, p. 1.
2 OJ L 119, 4.5.2016, p. 89.
3 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

– having regard to Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling of 23 November 2010[1],

– having regard to Opinion 7/2015 of the European Data Protection Supervisor of 19 November 2015 entitled 'Meeting the challenges of big data – A call for transparency, user control, data protection by design and accountability'[2],

– having regard to Opinion 8/2016 of the European Data Protection Supervisor of 23 September 2016 entitled 'EDPS Opinion on coherent enforcement of fundamental rights in the age of big data'[3],

– having regard to the statement of the Article 29 Data Protection Working Party on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU of 16 September 2014[4],

– having regard to Rule 52 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A8-0044/2017),

A. whereas big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics);

B. whereas certain big data use cases involve the training of artificial intelligence appliances, such as neuronal networks, and statistical models in order to predict certain events and behaviours; whereas the training data are often of questionable quality and not neutral;

C. whereas the progress of communication technologies and the ubiquitous use of electronic devices, monitoring gadgets, social media, web interactions and networks, including devices which communicate information without human interference, have led to the development of massive, ever-growing data sets which, through advanced processing techniques and analytics, provide unprecedented insight into human behaviour, private life and our societies;

D. whereas the intelligence services of third countries and Member States have increasingly been relying on the processing and analytics of such datasets, which are either not covered by any legal framework or, most recently, have been the subject of legislation the compatibility of which with Union primary and secondary law raises concerns and is yet to be ascertained;

---

1 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

2 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

3 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-23_BigData_opinion_EN.pdf

4 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

E. whereas the increase in bullying, violence against women and the vulnerability of children is also taking place on the internet; whereas the Commission and the Member States should adopt all the requisite legal measures to combat these phenomena;

F. whereas an increasing number of corporations, businesses, bodies and agencies, governmental and non-governmental organisations (as well as the public and private sectors in general), political leaders, civil society, academia, the scientific community and citizens as a whole have taken advantage of such data sets and big data analytics to bolster competitiveness, innovation, market predictions, political campaigns, targeted advertising, scientific research and policymaking in the field of transport, taxation, financial services, smart cities, law enforcement, transparency, public health and disaster response, and to influence elections and political outcomes through, for instance, targeted communications;

G. whereas the big data market is growing as a result of the technology and the process of data-driven decision-making being increasingly accepted as providing solutions; whereas there is not yet the methodology to make an evidence-based assessment of the total impact of big data, but there is evidence to suggest that big data analytics can have a significant horizontal impact across both the public and private sectors; whereas the Commission's Digital Single Market Strategy for Europe recognises the potential of data-driven technologies, services and big data to act as a catalyst for economic growth, innovation and digitalisation in the EU;

H. whereas big data analytics generates added value in a variety of ways, with numerous positive examples, entailing significant opportunities for citizens, e.g. in the areas of healthcare, the fight against climate change, the reduction of energy consumption, improvements to transport safety and the enablement of smart cities, thereby improving business optimisation and efficiency and contributing to improved working conditions and detecting and combating fraud; whereas big data can provide a competitive advantage to the decision-making processes of European companies, while the public sector can benefit from greater efficiency thanks to greater insights into the different levels of socio-economic developments;

I. whereas big data has the aforementioned potential for citizens, academia, the scientific community and the public and private sectors, but also entails significant risks, namely with regard to the protection of fundamental rights, such as the right to privacy, data protection and data security, but also freedom of expression and non-discrimination, as guaranteed by the EU Charter of Fundamental Rights and Union law; whereas pseudonymisation and encryption techniques can mitigate risks related to big data analytics and therefore play an important role in safeguarding the privacy of the data subject, while also fostering innovation and economic growth; whereas these elements are to be considered as part of the current revision of the e-privacy Directive;

J. whereas the pervasiveness of sensors, extensive routine data production and contemporary data-processing activities are not always sufficiently transparent, posing challenges to the capacity of individuals and authorities to assess the processes and purpose of the collection, compilation, analysis and use of personal data; whereas a blurring between personal and non-personal data can be seen to emerge from the use of big data analytics, which may lead to new personal data being created;

K. whereas the big data sector is growing by 40 % per year, seven times faster than the IT

market; whereas the concentration of large datasets produced by new technologies offers crucial information for large corporations, triggering unprecedented shifts in the balance of power between citizens, governments and private actors; whereas such concentration of power in the hands of corporations might consolidate monopolies and abusive practices and have a detrimental effect on consumers' rights and fair market competition; whereas the interests of the individual and the protection of fundamental rights should be further scrutinized in the context of big data mergers;

L. whereas big data has huge untapped potential as a driver of productivity and a means of offering better products and services to citizens; underlines, however, that the generalised use of smart devices, networks and web applications by citizens, businesses and organisations does not necessarily indicate satisfaction with the products offered, but rather a broader understanding that these services have become indispensable to live, communicate and work, despite a lack of understanding about the risks that they might pose to our well-being, security and rights;

M. whereas a distinction should be made between data quantity and data quality in order to facilitate the effective use of big data (algorithms and other analytical tools); whereas low-quality data and/or low-quality procedures behind decision-making processes and analytical tools could result in biased algorithms, spurious correlations, errors, an underestimation of the legal, social and ethical implications, the risk of data being used for discriminatory or fraudulent purposes and the marginalisation of the role of humans in these processes, leading to flawed decision-making procedures that have a detrimental impact on the lives and opportunities of citizens, in particular marginalised groups, as well as bringing about a negative impact on societies and businesses;

N. whereas algorithmic accountability and transparency should mean implementing technical and operational measures that ensure transparency, the non-discrimination of automated decision-making and the calculating of probabilities of individual behaviour; whereas transparency should give individuals meaningful information about the logic involved, the significance and the envisaged consequences; whereas this should include information about the data used for training big data analytics and allow individuals to understand and monitor the decisions affecting them;

O. whereas data analysis and algorithms increasingly impact on the information made accessible to citizens; whereas such techniques, if misused, may endanger fundamental rights to information as well as media freedom and pluralism; whereas the system of public broadcasting in Member States is directly related to the democratic, social and cultural needs of each society and to the need to preserve the plurality of the media, as stated in the Protocol on the system of public broadcasting in the Member States to the Amsterdam Treaty (11997D/PRO/09);

P. whereas the proliferation of data processing and analytics, the sheer number of actors involved in collecting, retaining, processing, storing and sharing data and the combination of large data sets containing personal and non-personal data from a variety of sources, while entailing significant opportunities, have all created great uncertainty for citizens and the public and private sectors alike over the specific requirements for compliance with current EU data-protection law;

Q. whereas there is a plethora of unstructured legacy systems containing vast volumes of data collected by companies over many years, with unclear data governance systems

that should be systematically brought into compliance;

R. whereas closer cooperation and coherence between different regulators and supervisory competition, consumer protection and data protection authorities at national and EU level should be encouraged, in order to ensure a consistent approach to and understanding of the implications of big data for fundamental rights; whereas the establishment and further development of the Digital Clearing House[1] as a voluntary network of enforcement bodies can contribute to enhancing their work and their respective enforcement activities and can help deepen the synergies and the safeguarding of the rights and interests of individuals;

General considerations

1. Stresses that the prospects and opportunities of big data can only be fully tapped into by citizens, the public and private sectors, academia and the scientific community when public trust in these technologies is ensured by a strong enforcement of fundamental rights and compliance with current EU data protection law and legal certainty for all actors involved; stresses that the processing of personal data can only be done pursuant to any of the legal bases laid down in Article 6 of Regulation (EU) 2016/679; considers that it is crucial that transparency and the proper provision of information to the audiences concerned are key to building public trust and to the protection of individual rights;

2. Underlines that compliance with the existing data protection legislation, together with strong scientific and ethical standards, are key to establishing trust in and the reliability of big data solutions; further emphasises that information revealed by big data analysis does not offer an impartial overview of any subject matter and is only as reliable as the underlying data permits; highlights that predictive analysis based on big data can only offer a statistical probability and therefore cannot always accurately predict individual behaviour; stresses, therefore, that strong scientific and ethical standards are vital for managing data collection and judging the results of such analysis;

3. Points out that sensitive information about persons can be inferred from non-sensitive data, which blurs the line between sensitive and non-sensitive data;

4. Stresses that individuals' poor knowledge and understanding about the nature of big data allows personal information to be used in unintended ways; notes that education and awareness about fundamental rights is of primary importance in the EU; urges the EU institutions and Member States to invest in digital literacy and awareness-raising about digital rights, privacy and data protection among citizens, including children; underlines that such education should address the understanding of the principles/logic of how algorithms and automated decision-making processes work and how to meaningfully interpret them; stresses, moreover, the need to educate with a view to fostering understanding on where and how data streams are collected (i.e. web scraping, combining streaming data with data from social networks and connected devices and aggregating that information into a new data stream);

Big data for commercial purposes and in the public sector

---

[1] Opinion 8/2016 of the European Data Protection Supervisor of 23 September 2016, p. 15.

Privacy and data protection

5. Points out that Union law on the protection of privacy and personal data, the right to equality and non-discrimination, as well as the right of individuals to receive information about the logic involved in automated decision-making and profiling and the right to seek judicial redress are applicable to data processing when processing is preceded by pseudonymisation techniques or, in any case, when the use of non-personal data might impact on individuals' private lives or other rights and freedoms, leading to the stigmatisation of whole groups of the population;

6. Underlines that the Digital Single Market must be built on reliable, trustworthy and high-speed networks and services that safeguard the fundamental rights of the data subject to data protection and privacy, while also encouraging innovation and big data analytics in order to create the right conditions and a level playing field to boost the European digital economy;

7. Further highlights the possibility of re-identifying individuals by correlating different types of anonymised data; underlines that Union law for the protection of privacy and personal data applies to the processing of such correlated data only when an individual is indeed re-identifiable;

8. Stresses that the aforementioned principles should serve as a framework for the decision-making procedures of the public and private sectors and other actors that use data; emphasises the need for much greater algorithmic accountability and transparency with regard to data processing and analytics by the private and public sectors and any other actors using data analytics, as an essential tool to guarantee that the individual is appropriately informed about the processing of their personal data;

9. Highlights the fundamental role that the Commission, the European Data Protection Board, national data protection authorities and other independent supervisory authorities should play in the future to promote transparency and due process, legal certainty in general and, more specifically, concrete standards that protect fundamental rights and guarantees associated with the use of data processing and analytics by the private and public sector; calls for closer collaboration among regulators of conduct in the digital environment, so as to strengthen the synergies between regulatory frameworks for consumers and competition and data protection authorities; calls for adequate funding and staffing of such authorities; acknowledges, moreover, the need for the establishment of a Digital Clearing House;

10. Underlines that the intrinsic purpose of big data should be to achieve comparable correlations with as few personal data as possible; stresses, in this regard, that science, business and public communities should focus on research and innovation in the area of anonymisation;

11. Recognises that the application of pseudonymisation, anonymisation or encryption to personal data can reduce the risks to the data subjects concerned when personal data are used in big data applications; further highlights the advantages of pseudonymisation provided for by the GDPR as an appropriate safeguard; recalls that anonymisation is an irreversible process by which personal data can no longer be used alone to identify or single out a natural person; takes the view that contractual obligations should ensure that anonymised data will not be re-identified using additional correlations by

combining different data sources; calls on the private and the public sector and other actors involved in the analysis of big data to regularly review such risks in the light of new technologies and to document the appropriateness of the measures adopted; calls on the Commission, the European Data Protection Board and other independent supervisory authorities to prepare guidelines on how to properly anonymise data in order to avoid future abuses of these measures and to monitor practices;

12. Urges the private and public sectors and other data controllers to make use of instruments provided for by the GDPR, such as codes of conduct and certification schemes, in order to seek greater certainty over their specific obligations under Union law and to bring their practices and activities into compliance with the appropriate EU legal standards and safeguards;

13. Calls on the Commission and Member States to ensure that data-driven technologies do not limit or discriminate access to a pluralistic media environment, but rather foster media freedom and pluralism; emphasises that cooperation between governments, educational institutions and media organisations will play a pivotal role in ensuring that digital media literacy is supported in order to empower citizens and protect their rights to information and freedom of expression;

14. Takes the view that the publication of personal data by public authorities for reasons of public interest, such as the prevention of corruption, conflicts of interest, tax fraud and money laundering, may be admissible in a democratic society, provided that the data is disclosed pursuant to conditions laid down by the law, that the appropriate safeguards are in place and that such publication is necessary for and proportionate to the desired aimed;

Security

15. Recognises the added value of the technological development that will contribute to improving security; acknowledges that some of the most pressing risks associated with data processing activities, such as big data techniques (especially in the context of the Internet of things), which are a matter of concern for individuals, include security breaches, unauthorised access to data and unlawful surveillance; believes that tackling such threats without abusing fundamental rights requires genuine and concerted cooperation between the private and public sectors, law enforcement authorities and independent supervisory authorities; stresses, in this regard, that specific attention should be paid to the security of e-government systems, as well as to additional legal measures such as software liability;

16. Takes the view that the use of end-to-end encryption should also be encouraged and, where necessary, mandated in accordance with the principle of data protection by design; recommends that any future legislative framework to this end specifically prohibits encryption providers, communications service providers and all other organisations (at all levels of the supply chain) from allowing or facilitating ‘backdoors’;

17. Highlights that heightened data generation and data flows entail further vulnerabilities and new information security challenges; calls, in this context, for the use of privacy by design and default, anonymisation techniques where appropriate, encryption techniques, and mandatory privacy impact assessments; stresses that such measures should be

applied by all actors involved in big data analytics in the private and public sectors and other actors dealing with sensitive data, such as lawyers, journalists and people working in the health sector so as to ensure that big data does not increase exposure to information security risks;

18. Recalls that in accordance with Article 15 of Directive 2000/31/EC, Member States shall neither impose a general obligation on the providers of transmission, storage and hosting services to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances suggesting illegal activity; reiterates in particular that the Court of Justice of the European Union, in the cases C-360/10 and C-70/10, rejected measures for the 'active monitoring' of almost all users of the services concerned (internet access providers in one case, a social network in the other) and specified that any injunction requiring a hosting services provider to undertake general monitoring shall be precluded;

Non- discrimination

19. Stresses that, because of the data sets and algorithmic systems used when making assessments and predictions at the different stages of data processing, big data may result not only in infringements of the fundamental rights of individuals, but also in differential treatment of and indirect discrimination against groups of people with similar characteristics, particularly with regard to fairness and equality of opportunities for access to education and employment, when recruiting or assessing individuals or when determining the new consumer habits of social media users;

20. Calls on the Commission, the Member States and the data protection authorities to identify and take any possible measures to minimise algorithmic discrimination and bias and to develop a strong and common ethical framework for the transparent processing of personal data and automated decision-making that may guide data usage and the ongoing enforcement of Union law;

21. Calls on the Commission, the Member States and the data protection authorities to specifically evaluate the need not only for algorithmic transparency, but also for transparency about possible biases in the training data used to make inferences based on big data;

22. Recommends that businesses conduct regular assessments into the representativeness of data sets, consider whether data sets are affected by biased elements, and develop strategies to overcome those biases; highlights the need to review the accuracy and meaningfulness of data analytics predictions on the basis of fairness and ethical concerns;

Big Data for scientific purposes

23. Stresses that big data analytics can be beneficial for scientific development and research; believes that the development and use of big data analytics for scientific purposes should be conducted with due regard for the fundamental values enshrined in the Charter of Fundamental Rights and in compliance with current EU data protection legislation;

24. Recalls that under the GDPR, the further processing of personal data for statistical

purposes may only result in aggregate data which cannot be re-applied to individuals;

Big data for law enforcement purposes

Privacy and data protection

25. Reminds all law enforcement actors that use data processing and analytics that Directive (EU) 2016/680: governs the processing of personal data by Member States for law enforcement purposes; requires that the collection and processing of personal data for law enforcement purposes must always be adequate, relevant and not excessive in relation to the specified, explicit and legitimate purposes for which they are processed; states that the purpose of and need for the collection of these data must be clearly proven; states that any decision based solely on automated processing, including profiling, which produces an adverse legal effect on the data subject or significantly affects him or her, is prohibited, unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controllers; calls on the Commission, the European Data Protection Board and other independent supervisory authorities to issue guidelines, recommendations and best practices in order to further specify the criteria and conditions for decisions based on profiling and the use of big data for law enforcement purposes;

26. Stresses the importance of compliance with Directive (EU) 2016/680 as regards the carrying out of prior impact assessments and audits that take account of ethical concerns in order to assess the inclusiveness, accuracy and quality of data, and to ensure that individuals targeted by the decisions and/or actors involved in the decision-making processes are able to understand and challenge the collection or analysis, patterns and correlations and to prevent any harmful effects on certain groups of individuals;

27. Points out that the trust of citizens in digital services can be seriously undermined by government mass surveillance activities and the unwarranted accessing of commercial and other personal data by law enforcement authorities;

28. Recalls that legislation permitting public authorities to gain access to the contents of electronic communications on a generalised basis must be regarded as compromising the essence of the fundamental right to respect for one’s private life, as guaranteed by Article 7 of the Charter;

29. Stresses the need for guidelines and systems to be incorporated into public tenders for data processing models, tools and programmes based on big data for law enforcement purposes in order to ensure that the underlying code can be and is checked by the law enforcement authority prior to final purchase and can be verified for its suitability, correctness and security, bearing in mind that transparency and accountability are limited by proprietary software; points out that certain models of predictive policing are more privacy-friendly than others, such as where probabilistic predictions are made about places or events and not about individual persons;

Security

30. Underlines the absolute need to protect law enforcement databases from security breaches and unlawful access since this is a matter of concern for individuals; believes,

therefore, that tackling such risks requires concerted and effective cooperation between law enforcement authorities, the private sector, governments and independent supervisory data protection authorities; insists on the need to guarantee adequate security for personal data, in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680, as well as to minimise vulnerabilities through secured and decentralised database architectures;

Non-discrimination

31. Warns that, owing to the intrusiveness of the decisions and measures taken by law enforcement authorities – including by means of data processing and data analytics – into the lives and rights of citizens, maximum caution is required in order to prevent unlawful discrimination and the targeting of certain individuals or groups of people defined by reference to race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, property, birth, disability, age, gender, gender expression or identity, sexual orientation, residence status, health or membership of a national minority which is often the subject of ethnic profiling or more intense law enforcement policing, as well as individuals who happen to be defined by particular characteristics; calls for proper training for the frontline collectors of data and users of intelligence derived from the data analysis;

32. Calls on the Member States' law enforcement authorities that make use of data analytics to uphold the highest standards of ethics when analysing data and to ensure human intervention and accountability throughout the different decision-making stages, not only to assess the representativeness, accuracy and quality of the data, but also to assess the appropriateness of each decision to be taken on the basis of that information;

°

° °

33. Instructs its President to forward this resolution to the Council and the Commission.